Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8562904, 11 pages
https://doi.org/10.1155/2018/8562904

Research Article

A Security Scheme of 5G Ultradense Network Based on the Implicit Certificate

Zhonglin Chen,[1] Shanzhi Chen,[1,2] Hui Xu,[2] and Bo Hu[1]

[1] *State Key Lab of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *State Key Lab of Wireless Mobile Communication, China Academy of Telecommunications Technology, Beijing 100081, China*

Correspondence should be addressed to Zhonglin Chen; chenzl@263.net

Received 2 March 2018; Accepted 19 April 2018; Published 23 May 2018

Academic Editor: Fuhong Lin

The ultradense network (UDN) is one of the most promising technologies in the fifth generation (5G) to address the network system capacity issue. It can enhance spatial reuse through the flexible, intensive deployment of small base stations. A universal 5G UDN architecture is necessary to realize the autonomous and dynamic deployment of small base stations. However, the security of the 5G UDN is still in its infancy, and the data communication security among the network entities is facing new challenges. In this paper, we proposed a new security based on implicit certificate (IC) scheme; the scheme solves the security problem among the access points (APs) in a dynamic APs group (APG) and between the AP and user equipment (UE). We present each phase regarding how two network entities obtain the Elliptic Curve Qu-Vanstone (ECQV) implicit certificate scheme, verify each other's identity, and share keys in an UDN. Finally, we extensively analyze our lightweight security communication model in terms of security and performance. The simulation on network bandwidth evaluation is also conducted to prove the efficiency of the solution.

1. Introduction

In the 5G, data traffic will experience explosive growth in the years to come. The use of wireless physical layer technologies (e.g., coding technology, modulation technology, and multiple access technology) can only increase spectrum efficiency by about 10 times and the wider bandwidth can only improve the transmission efficiency by dozens of times. This is far from meeting the 5G demand. However, through the deployment of dense base stations, the spectrum efficiency caused by reducing the cell coverage radius can be increased by more than 2700 times [1]. Obviously, the application of dense small base stations with the narrow coverage in the heterogeneous network can remarkably improve the system capacity. In order to enhance up the system capacity of regional hotspot hundreds of times, the small bases network deployment needs to be more flexible and the frequency reuse needs to be more efficient. Therefore, the ultradense network (UDN) is proposed and has attracted wide attention [2].

The UDN is considered to be one of the most effective solutions to improve wireless system capacity. It decreases the distance between the user equipment (UE) and the network entities and greatly improves the spectrum efficiency. Meanwhile, the UDN has been identified as a constituent of future 5G core technologies by the IMT-2020 expert group [3]. With various small base stations acting as access points (APs), the intersite distance (ISD) decreases as the network entities' density increases. The AP of 5G is different from the traditional macro station. Traditional macro stations are regularly deployed by operators, while AP deployment may be irregular or even deployed by users. Pseudo or malicious AP will threaten 5G system security. What is more, the APs are not just an air network link; they will cooperate with each other to serve user in UDN. In the air transmission of UDN, the unprotected data among the APs is easy to intercept. Therefore, the mutual authentication and the secure data communication among the dense APs, including the keys for the sessions, will face new challenges.

As the wireless access network of the 5G, the UDN adopts a different deployment plan that focuses on the new requirement of "network follows user" and supports higher date transmission rates and multiple services. This must fully

Table 1: Comparison of the traditional certificate and implicit certificate.

Security level	Public key length (bits)		Certificate length (bits)			ECQV/RSA
	ECC	RSA	ECQV	ECDSA	RSA	
80	192	1024	193	577	2048	9.42%
112	224	2048	225	673	4096	5.49%
128	256	3072	257	769	6144	4.18%
192	384	7680	385	1153	15360	2.51%
256	521	15360	522	1564	30720	1.70%

support the organization and access security of dense APs in a heterogeneous environment and also support the seamless connectivity of the user-to-AP, AP-to-AP, and machine-to-machine communications. Therefore, the UDN faces more extensive and complex security threats than traditional wireless systems. However, the security research of the 5G UDN is still in an initial stage, especially the data communication security among the network entities.

In this paper, we propose a new security scheme based on implicit certificate (IC) to solve the security issues among the dense deployment access points (APs) in a dynamic APs group (APG) and between the AP and user equipment (UE). As a new variant of the public key certificate, the novel IC is more efficient in computing and bandwidth allocation, and it requires no peer information before a secure data communication session [4]. The IC has been widely applied to the efficient authentication of resource-constrained Internet of Things (IoT) systems in the literature [5, 6]. Meanwhile, based on the IC, [7] proposed an effective public key infrastructure for the Vehicle-to-Grid Network. After in-depth research, we believe that the principle based on the IC is suitable for providing a security solution for the UDN.

A new lightweight security scheme for secure data communications is presented in this paper. We provide the specific implementation solutions for the security application scenes in the UDN. Meanwhile, the security scheme is analyzed, and the simulation of the network bandwidth evaluation is conducted to prove the efficiency of the solution. Specifically, the scheme focuses on solving the following three subissues:

(i) How to generate the IC and private key

(ii) How to implement the mutual authentication based on the IC among the network entities

(iii) How to implement the lightweight secure communication with a shared key based on the IC

The main contributions of our proposed scheme are summarized as follows:

(i) In our solution, the reconstructed private key that would be instantaneously generated based on the IC could solve the key security issues in actual operations.

(ii) We propose an innovative scheme to solve the security issues of data communications by using shared key encryption based on the IC.

(iii) Our innovative authentication and key agreement method based on the IC is lightweight, efficient, and less resource-consuming.

The rest of the paper is organized as follows. In Section 2, the security challenges in the 5G UDN architecture are analyzed. The implicit certificate and relevant background knowledge are presented in Section 3. The design of the security solution based on the IC and the implementation processes are described in Section 4. Then, the security analysis and performance evaluation are presented in Section 5. The final conclusions are drawn in Section 6.

2. Implicit Certificate and Related Work

Compared with the traditional digital certificate based on the public key infrastructure (PKI) [8, 9], the implicit certificate (IC) [10] has significant advantages.

The traditional digital certificate (the explicit certificate) is a fixed structure that binds the public key (expressed as P) with the identity (expressed as I) that has an attached signature (expressed as Sig) that can be expressed as a triple (I, P, and Sig) [11, 12]. Different from the traditional certificate, the IC is composed of an identity element (still expressed as I) and reconfigurable key data (also expressed as P). P can reconstruct the public key of the identity entity together with the public key of the certificate authority (CA) [13]. Then, the IC could be expressed as a two-tuple (identity element and reconstructed key data) such as (I, P). Traditional authentication uses the RSA (Rivest-Shamir-Adleman algorithm) [14], the ECDSA (Elliptic Curve Digital Signature Algorithm), and other solutions to conduct the signature process, while the typical implicit authentication adopts the ECQV (Elliptic Curve Qu-Vanstone) solution [15].

(A) Smaller Size and Less Bandwidth Occupation. The IC can reduce the bandwidth occupation in the transmission process. Therefore, it is quite suitable for mobile communications, the Internet of Things (IoT), and other resource-constrained environments. Table 1 shows that the traditional digital certificate (such as the RSA) requires more bandwidth than the IC that uses the lightweight Elliptic Curves Cryptography (ECC) cryptosystem [16, 17]. For example, when the security level in a practical application is 112 bits, the IC size is merely 225 bits, which is 43% of the ECDSA certificate (673 bits) and 5.5% of the RSA certificate (4096 bits).

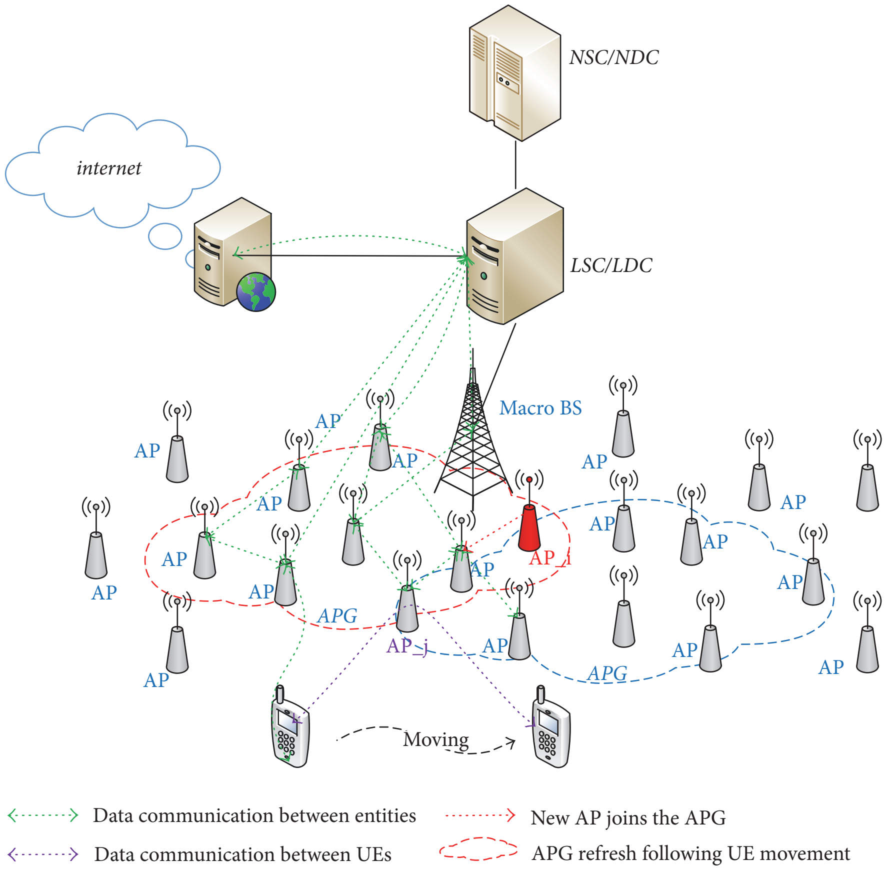


Figure 1: Typical UDN/UUDN architecture.

(B) Higher Speed and Less Resource Consumption. The IC takes the reconstructed public key as a substitute for the signature authentication process. It requires less computing resources compared to a traditional certificate. In addition, some handlers can be integrated into a parallel process with subsequent communication protocols. This may further reduce the computing time and improve efficiency.

In the implicit certificate, there is no signature process instead of the reconstructed public key. The computing work of the reconstructed public key is very small. Then, the implicit certificate is faster than the traditional certificate, consumes fewer resources, and also has better security [18]. For example, when a user's cell phone is stolen, then his private key will also be lost. In the traditional certificate, users need to apply for his certificate revocation to CA. The traditional certificate revocation is to publish the certificate revocation list (CRL) periodically. In large-scale network environment, the CRL is usually large. Because of the periodicity of CRL, the user certificate revocation will be delayed certainly. Thus, the user data security will be threatened. However, the implicit certificate is different. The user's private key corresponds to a short-term lightweight implicit certificate [19]. It does not need to be revoked. And it can be issued quickly and temporarily. In this way, the user's data communication will be more secure. Therefore, the implicit certificate shows stronger advantages than the traditional certificate. For example, ECQV based on implicit certificate has been successfully applied to the field of ZigBee wireless communication. It can be predicted that the implicit certificate can be more widely applied to mutual authentication and secure communication among the network entities in 5G system.

3. UDN Architecture and Security Challenges

3.1. Ultradense Network Architecture. The typical application scenarios of the UDN include office districts, intensive residential areas, high-density blocks, campuses, large gatherings, stadiums, subways, and apartments [20]. The above scenarios require the network to be deployed with adequate flexibility, efficiency, intelligence, and integration abilities. According to practical application demands, different UDN architectures are designed using various organizations of different base stations.

One type of UDN is based on the static virtual cell, which is composed of multiple access points in the area to form a "large" static cell and can provide users a similar coverage to that of the macro base station service experience with a unified identity and common services [21].

Another type of UDN is the user-centric UDN (UUDN) [22, 23], which has a local control center coordinated with the user, and the virtual adjoined cell is defined based on the unit of a single user. A typical UDN/UUDN architecture is shown in Figure 1. In the UUDN, the system organizes a dynamic APs group (APG) that depends on each UE's situation. It provides unaware and seamless service to the user through dynamic refreshing of the APG as an invisible network coverage accompanying user movement.

3.2. Security Challenges in UDN. The 5G network confronts more extensive and complex security threats compared to current 3G and 4G networks. It includes the traditional security threats in the mobility of multiple UEs and the openness of the wireless channel. Moreover, it also includes new security threats from the enhanced functionality in multiple use patterns, the integration between diversified heterogeneous wireless networks, the open network infrastructure based on the IP framework, and the enriched business bearer with different trust-ratings [24].

The security problems of data communication in the UDN could be summarized as follows.

(C) Access Authentication Security for UE to UDN. To ensure access security, network access authentication is required for the UE to connect with the 5G network. Different from that of the 3G and 4G networks with traditional macro base station coverage, the security threat of UDN cannot be fully avoided by solely depending on traditional authentication and key agreements (AKAs) [25, 26]. For example, the network entities of the UDN in the flexible deployment environment (such as user self-deployed AP or an uncontrolled deployment environment) can be hijacked. Therefore, the security of UE authentication shall be strengthened.

The UE delivers an initial access request. Then, the AP receives the request and transmits it to the local network system. In accordance with the request's context, the local network system requests that the core network system provide the corresponding network layer authentication vector and response. Then, on the basis of the received network layer security parameter, the local network system initiates the network layer's mutual authentication process with the UE (similar to the 4G EPS-AKA process). When the network layer mutual authentication of the UE is finished, a static virtual cell or an APG is allocated to the UE by the UDN. At this time, the local network system generates network access authentication vectors to the UDN control layer based on the request parameter submitted from the UE. It conducts the access layer (a specific virtual cell or APG) mutual authentication process on the UE. When the mutual authentication processes toward both the network layer and the access layer are finished by the UE, the security access is accomplished.

(D) Communication Security among APs/APG. The UDN is composed of densely deployed APs. The APs are connected and organically organized depending on different technical framework demands, such as a unified static virtual cell or an APG. Regardless of the AP organization, the UDN must realize the access service of the UE while maintaining a high-quality user experience. Therefore, the influential factors should be eliminated in the UDN, such as the cochannel interference, shared spectrum interference, interference between multiple coverage layers and frequent network handover caused by the density increase, or the distance decrease between base stations [27].

To protect the APs from various security threats caused by other APs (e.g., illegal APs or malicious APs) and build a secure UDN environment, a solution for secure data communications between APs is necessary and very important. Furthermore, because of the limited capability and small coverage of APs different from the traditional macro base station in 3G and 4G networks, the security of data communication faces new challenges.

(E) Communication Security between UE and AP/APG. With the intelligent development of the UE, network data transportation is getting flatter. Several new trends have emerged in the 5G network architecture, including the localized flat, heterogeneous coordination of macro and small base stations, and submerging business functions. APs and APG are more than a network access. Depending on the difference in the APs and APG functional requirement, they can realize data transportation, data control, or both. The APs or APG becomes the key network entity when the UE accesses the 5G system and Internet. If the relevant registration data suffers security attacks, the security of user traffic also encounters risks. Therefore, the data communication security between users and APs (or APGs) is another security challenge for the 5G UDN.

Based on this analysis, the security requirements of data communication in the UDN include the following:

(i) Each network entity should be mutually authenticated, and the bilateral entities should use their respective private keys. The security mechanism should be applied to ensure that both sides can receive relevant information.

(ii) Each communication entity should be able to obtain the shared keys in data communications. The different communication sessions use different shared keys.

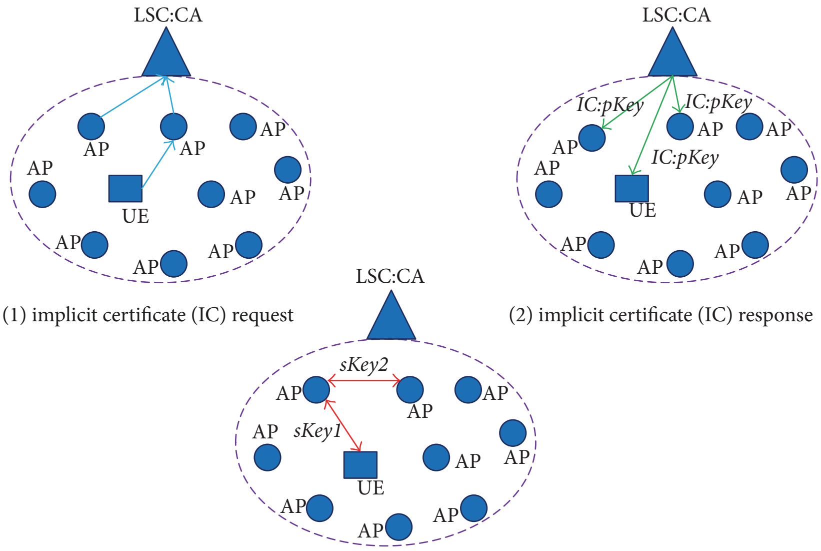
(iii) The security mechanisms for data encrypted based on shared keys should support the dynamic joining or leaving of communication entities.

(iv) All entities should receive unified management from the network operator. The generation of shared keys between communication entities should be in accordance with the relevant instructions.

(v) The security mechanism should support multiple logical channels between the same sources or destinations and avoid the duplication of the keystream.

(vi) The security mechanism should be efficient to ensure quick responses and adapt to the entity's performance and network bandwidth in different communication processes.

From the above requirements, a new certificate and key agreement mechanism are required to establish a secure connection for each pair of entities. Therefore, we propose a new security scheme based on the IC to implement the lightweight data communication between various entities.



(1) implicit certificate (IC) request

(2) implicit certificate (IC) response

(3) Secure communication between entities

(1) APs/UE: its own private key (pKey) can be reconstructed
(2) the shared key (sKey, between AP and AP or between AP and UE) is instant by the algorithm computing

Figure 2: Communication between entities in a UDN based on the IC.

4. UDN Security Solution

The data communication among network entities can be described as follows. It is based on the digital certificate and entity-to-entity security data communication model with the participation of the local service center. The entity can be AP or UE. The local service center (LSC) could run within CA functions.

4.1. Security Model and Notations. Data communication among the network entities is temporary and random, such as when an AP dynamically joins or leaves an APG and when the UE temporarily accesses the APG or other network entities. Therefore, using the IC in temporary key generation is a more convenient and efficient solution to achieve a secure data communication session than the prefixed key distribution. Based on the reconstructed public key and private key, trusted authentication management and shared key generation can be implemented through the implicit certificate from the CA. Then, secure data communication sessions can be implemented by using the shared key computed by the network entities' participants.

Under a CA domain, there are three phases among communication entities. In Phase 1, the CA issues an IC to the requesting entity, which is called the phase of IC generation. In Phase 2, entities conduct mutual certification based on the IC, which is called the phase of mutual identity authentication. In Phase 3, entities exchange data based on shared keys, which is called the phase of shared key generation and data communication. The security data communication model based on the IC is shown in Figure 2.

We assume that the basic configuration has been uniformly predeployed at the initialization phase, including the elliptic curve (EC) parameters, the authentication key K, the public key Q_{CA} of the CA, and the unique user identity label I. The CA can verify the identity and validity of the network entities in order to decide whether they belong to its CA domain. The IC is an ECQV certificate in our solution. The network entities can directly transmit data or forward them through other entities (via single hop or several hops). Any entity can destroy the public key or identity I (or put it on the blacklist) according to the control demand of the LSC.

The notations used in this paper are defined in "Notations." The EC parameters are denoted using q, a, b, G, and n. q is a prime defined on the finite field Fq. a and b are coefficients of the EC curve: $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Another prime G is the base point generator of the EC with order n.

4.2. Security Algorithm Solution. To establish a secure data communication session among the network entities, the security solution based on the IC can be implemented in four phases.

Phase 1 (implicit certificate generation). Before establishing the secure data communication, the entities should launch an IC request to the CA. For example, a new AP (denoted as Ent_U) attempts to join the APG, where another entity (denoted as Ent_V) is registered. The entity Ent_U must communicate with the entity Ent_V and exchange essential information. Then, Ent_U sends an IC request message.

The entity Ent_U with a unique identity ID_U generates a random number r_U and computes $R_U = r_U * G$. Concurrently, to avoid a replay attack, Ent_U produces a cryptographic random number N_U and computes $\mathrm{HMAC}[K, R_U \parallel N_U \parallel \mathrm{ID}_U]$. Then, Ent_$U$ sends R_U, N_U, and ID_U as well as the value of HMAC to the CA. The HMAC is a keyed-hash message authentication code algorithm in cryptography.

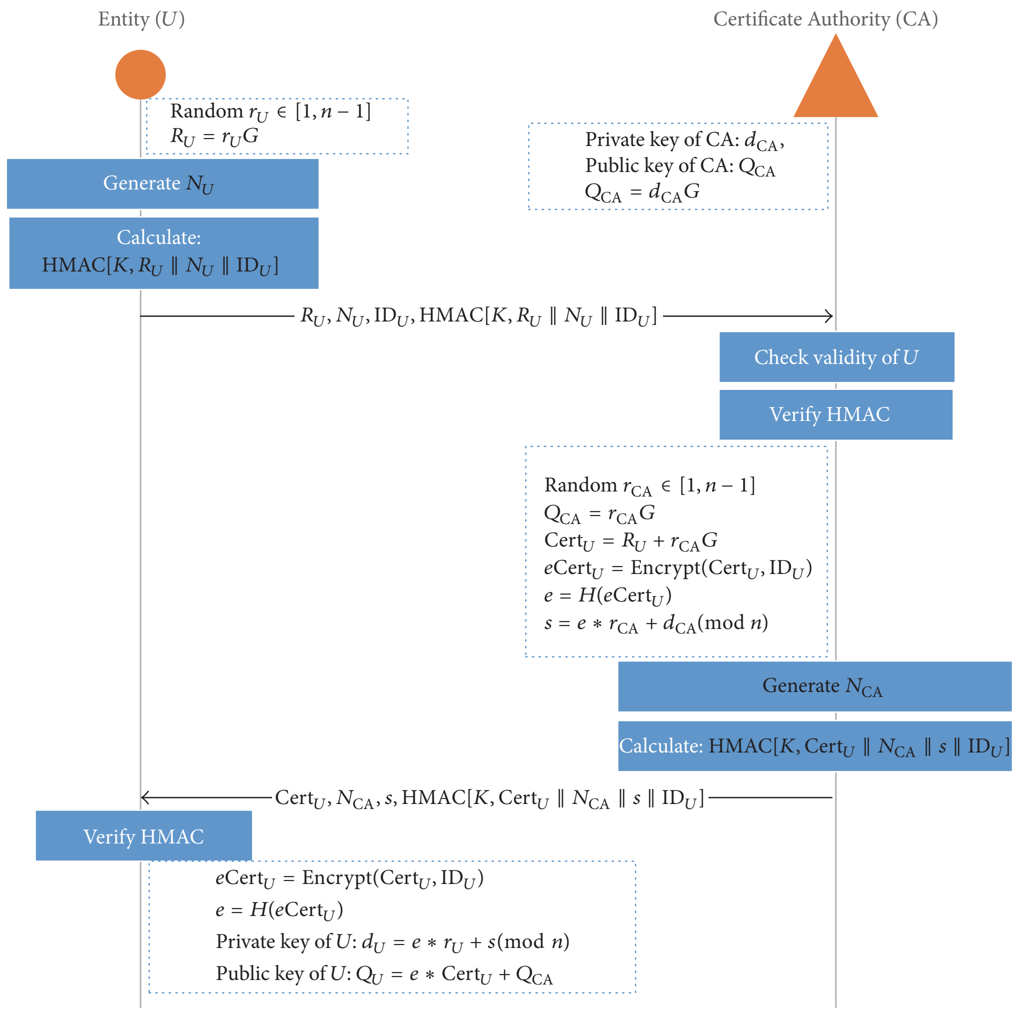

Entity (U)
Certificate Authority (CA)
Random $r_U \in [1, n-1]$
$R_U = r_U G$
Private key of CA: d_{CA},
Public key of CA: Q_{CA}
$Q_{CA} = d_{CA} G$
Generate N_U
Calculate:
HMAC$[K, R_U \parallel N_U \parallel ID_U]$
R_U, N_U, ID_U, HMAC$[K, R_U \parallel N_U \parallel ID_U]$
Check validity of U
Verify HMAC
Random $r_{CA} \in [1, n-1]$
$Q_{CA} = r_{CA} G$
$Cert_U = R_U + r_{CA} G$
$eCert_U = Encrypt(Cert_U, ID_U)$
$e = H(eCert_U)$
$s = e * r_{CA} + d_{CA} (\text{mod } n)$
Generate N_{CA}
Calculate: HMAC$[K, Cert_U \parallel N_{CA} \parallel s \parallel ID_U]$
$Cert_U, N_{CA}, s$, HMAC$[K, Cert_U \parallel N_{CA} \parallel s \parallel ID_U]$
Verify HMAC
$eCert_U = Encrypt(Cert_U, ID_U)$
$e = H(eCert_U)$
Private key of U: $d_U = e * r_U + s (\text{mod } n)$
Public key of U: $Q_U = e * Cert_U + Q_{CA}$

Figure 3: The generation process of the implicit certificate.

After the request is received, the CA (private key is d_{CA}, public key is Q_{CA}, and $Q_{CA} = d_{CA} * G$) verifies the identity ID_U and corresponding HMAC of Ent_U. If the validation is confirmed, a random number $r_{CA} \in [1, n-1]$ will be generated. The CA begins to compute the following:

(i) The reconstructed data of the public key: $Cert_U = R_U + r_{CA} * G$.

(ii) The encrypted certificate with the entity's identity: $eCert_U = Encrypt(Cert_U, ID_U)$, where ID_U is the entity's identity and Encrypt is an encoding function for the identity information protection.

(iii) The component data of the private key: $s = e * r_{CA} + d_{CA} (\text{mod}\, n)$, where $e = H(eCert_U)$. H is a Secure Hash Algorithm (SHA) such as SHA-1.

(iv) Similarly, a sequence code N_{CA} is generated by the CA, and then the CA sends back to the requester Ent_U with $Cert_U$, N_{CA}, s, and HMAC$[K, Cert_U \,||\, N_{CA} \,||\, s \,||\, ID_U]$.

Ent_U then verifies the message received from the CA. If the verification is confirmed, Ent_U computes the following keys using the reconstruction data:

$$\text{Ent\_}U \text{ private key (pKey): } d_U = e * r_U + s (\text{mod } n)$$

$$\text{Ent\_}U \text{ public key (PKey): } Q_U = e * Cert_U + Q_{CA}$$

At this point, entity Ent_U has its own public key and private key pair (d_U, Q_U) securely through the IC generation process. Similarly, other entities can apply for their respective ICs and the pairwise key, which is shown in Figure 3.

Phase 2 (mutual authentication between Ent_U and Ent_V). Similarly, the private key (pKey) $d_V = e * r_V + s (\text{mod}\, n)$ and public key (PKey) $Q_V = e * Cert_V + Q_{CA}$ of entity Ent_V can be easily obtained. Since the reconstructed data are publicly transmitted over the network in the UDN, other entities can be easily obtained.

Therefore, as long as the entity IC and its identity ID_U are known, it is easy to compute the entity's public key. Of course, the CA computes the IC and therefore obviously owns

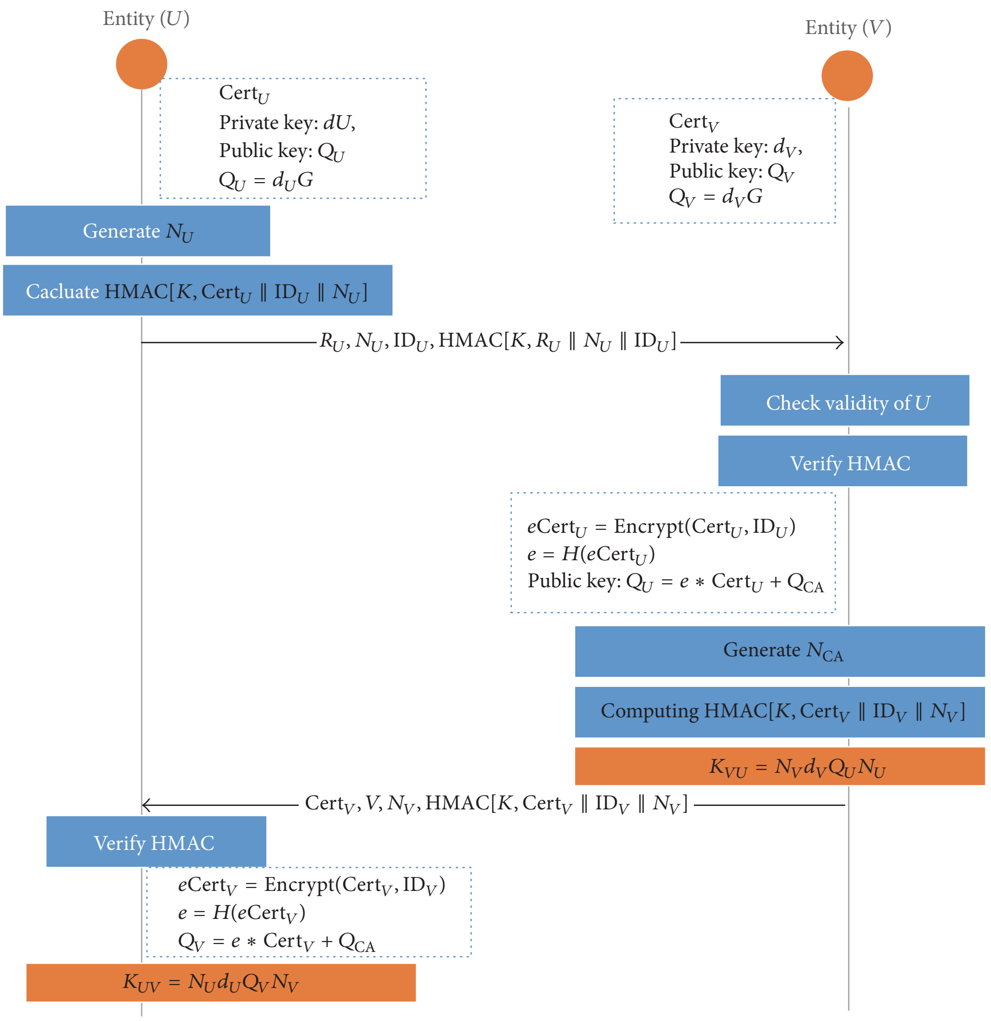

Entity (U)
Entity (V)
Cert_U
Private key: dU,
Public key: Q_U
$Q_U = d_U G$
Cert_V
Private key: d_V,
Public key: Q_V
$Q_V = d_V G$
Generate N_U
Calcuate $\mathrm{HMAC}[K, \mathrm{Cert}_U \parallel \mathrm{ID}_U \parallel N_U]$
$R_U, N_U, \mathrm{ID}_U, \mathrm{HMAC}[K, R_U \parallel N_U \parallel \mathrm{ID}_U]$
Check validity of U
Verify HMAC
$e\mathrm{Cert}_U = \mathrm{Encrypt}(\mathrm{Cert}_U, \mathrm{ID}_U)$
$e = H(e\mathrm{Cert}_U)$
Public key: $Q_U = e * \mathrm{Cert}_U + Q_{\mathrm{CA}}$
Generate N_{CA}
Computing $\mathrm{HMAC}[K, \mathrm{Cert}_V \parallel \mathrm{ID}_V \parallel N_V]$
$K_{VU} = N_V d_V Q_U N_U$
$\mathrm{Cert}_V, V, N_V, \mathrm{HMAC}[K, \mathrm{Cert}_V \parallel \mathrm{ID}_V \parallel N_V]$
Verify HMAC
$e\mathrm{Cert}_V = \mathrm{Encrypt}(\mathrm{Cert}_V, \mathrm{ID}_V)$
$e = H(e\mathrm{Cert}_V)$
$Q_V = e * \mathrm{Cert}_V + Q_{\mathrm{CA}}$
$K_{UV} = N_U d_U Q_V N_V$

FIGURE 4: The AKA-IC process for the shared key.

the public keys of all network entities. Any network entity can obtain the other entity's PKey from the CA, but it cannot obtain the pKey owned and computed by others.

The PKey of the entity Ent_U generated in Phase 1 can be verified by the CA. In other words, the identity of entity Ent_U can be verified by the CA using the following formulas:

$$\begin{aligned} Q_U = d_U * G &= (e * r_U + s \,(\mathrm{mod}\ n)\,(\mathrm{mod}\ n)) * G \\ &= (e * r_U + e * r_{\mathrm{CA}} + d_{\mathrm{CA}}\,(\mathrm{mod}\ n)) * G \\ &= e * (r_U + r_{\mathrm{CA}}) * G + d_{\mathrm{CA}} * G \\ &= e * (R_U + r_{\mathrm{CA}} * G) + Q_{\mathrm{CA}} = e * \mathrm{Cert}_U + Q_{\mathrm{CA}} \end{aligned} \quad (1)$$

The verification of Ent_V can also be similarly conducted.

In the UDN, a mutual challenge-response among the APs can be processed using the verification formula method.

Phase 3 (shared key generation between Ent_U and Ent_V). After the identities are confirmed, the entities can agree with the shared key for the communication session to guarantee the confidentiality of data transmission. The sender has to encrypt the data before transmission, while the receiver has to decrypt the data. Accordingly, both of the communication partners must have the same key, namely, the "shared" key (sKey), in this paper. However, since any data with the shared key can be intercepted and have high risk, it is impossible to transmit the key as plaintext in the network. Furthermore, each communication session is temporary and uncertain. The dynamic sessions require the key to be continuously refreshed and updated. It is difficult to preload different encryption keys for each communication session in the actual operator.

Fortunately, we discovered a lightweight scheme based on the IC to solve the issues mentioned above. The shared keys known only by both of the communication partners can be instantly generated through the authentication and key agreement protocol based on the IC (AKA-IC). Moreover, the shared key is locally generated and does not need to be transferred in the network. The new generation mechanism is shown in Figure 4.

From Phases 1 and 2, we know that the parameters of Cert_U, ID_U, N_U, and $\mathrm{HMAC}[K, \mathrm{Cert}_U \ || \ N_U \ || \ \mathrm{ID}_U]$ can be generated and sent to Ent_$V(d_V, Q_V)$ from Ent_$U(d_U, Q_U)$.

After entity Ent_V receives the message from Ent_U, it verifies the identity ID_U and HMAC. First, the public key Q_U of Ent_U can be computed by Ent_V. Then, Ent_V locally computes out the "shared" key sKey $= K_{VU}$ using its private key pKey d_V:

$$\mathrm{sKey} = K_{VU} = N_V d_V Q_U N_U \tag{2}$$

Similarly, the partner Ent_U locally computes the "shared" key sKey $= K_{UV}$ at the same time:

$$\mathrm{sKey} = K_{UV} = N_U d_U Q_V N_V \tag{3}$$

The equation can be derived as follows:

$$\begin{aligned}\mathrm{sKey} &= K_{UV} = N_U d_U Q_V N_V = N_V d_U Q_V N_U \\ &= N_V d_U \left(d_V G\right) N_U = N_V d_V \left(d_U G\right) N_U \\ &= N_V d_V Q_U N_U = K_{VU}\end{aligned} \tag{4}$$

Proof is finished.

The above equation of $K_{VU} = K_{UV} =$ sKey shows that the keys temporarily generated by two entities separately are the same, and they can realize secure data communications using the "shared" key sKey.

Phase 4 (secure communication between Ent_U and Ent_V). When Ent_U and Ent_V have their own pairwise key, the two entities can generate the shared key for their communication sessions. Ent_U encrypts the data that need to be protected by the shared key and sends them to Ent_V. After the encrypted data are received, Ent_V securely decrypts them. Then, the two entities enter into a secure interaction phase until the session ends.

5. Security Analysis and Performance Evaluation

Focusing on the sensing characteristics of randomly deployed MSNs, we analyzed the coverage redundancy problem for the MSNs, where the sensing ranges satisfy the normal distribution.

5.1. Security Analysis

(A) Security of Key Generation. The core of asymmetric cryptography security is the public/private key pair, especially the user's private key. In our solution, the CA generates the user's private key data that can reconstruct the IC using its trusted private key. Then, the reconstructed key data can be locally recomputed. Then, the actual user's private key is generated. The user's private key is locally generated and is not plaintext transmitted in the network. Thus, the security of the user's private key generation is ensured.

(B) Data Confidentiality in Transmission. In our solution, when network entities need to transmit data, both of the communication entities use their private/public key pairs to generate a shared key at their respective locations. The sender encrypts the data using the shared key and sends them to the opposite side. The receiver uses the agreed algorithm to generate the same key to decrypt the data. Thus, the confidentiality of data transmission between the communication entities is guaranteed.

(C) Antireplay Attack. In the process of the shared key generation, the antireplay attack factor NUNV (or timestamp) is added during each computation. If the current interactive data are intercepted and returned to the receiver, the receiver will identify and refuse to receive them. Each communication session has a different encryption key. Moreover, in order to ensure the freshness of shared keys, the secret number increases in the process. It can effectively reduce the shared key's break probability and ensure that the shared key cannot be temporarily reused in the transmission.

(D) Mutual Authentication. In our algorithm, both sides of the communication network's entities have to pass the authentication before they interact with each other. Before the sender delivers the data (such as random numbers and identities), the data must be signed with a digital signature using the sender's private key. When the receiver obtains the signed data, it will use the sender's public key to verify the data. Furthermore, the sender's public key is computed based on the reconstructed public key data. If the validation is correct, then the sender's identity is legal. Similarly, when the receiver sends a reply message, the reply vector data including the identity will also be signed. The opposite side conducts the same legal validation to the vector data. If both sides pass the opposite verification, mutual authentication is complete.

(E) Nonrepudiation. In the algorithm process, both of the communication entities sign the messages using the sender's private key. The source of the data can be identified through the signature, since only the owner of the private key can generate the signature. The receiver simply uses the sender's public key to verify the source of the message. Since the sender's private key is only known by the sender himself/herself, it can effectively prevent the middleman attack and ensure that the sender cannot deny the delivered messages.

(F) Anti-Denial-of-Service Attack. In our scheme, the CA verifies the identity based on the inspection mechanism. According to the registration information in the database, the CA starts with identity check, including blacklists. The CA will directly reject the unregistered or blacklisted user's application for implicit certificates. Therefore, the Denial-of-Service attacks from some malicious network entities are resisted in the UDN.

5.2. Performance Evaluation. In the practical application environment of the UDN, there are convenient deployment sites for small stations, such as large squares, and they may be limited by topography, such as blocks, stations, and other small stations that are irregularly deployed. Therefore, there are two deployment modes in our simulation: random deployment and regular deployment. To get closer to the

Table 2: Frequency of handover.

Simulation scene (320 ∗ 320 m^2)	UE's speed (km/h)	Handover (times/second/user)
Scene 1: APs randomly deployed, L2 centralized	3	0.731
	30	1.421
	60	2.018
Scene 2: APs randomly deployed, L1 centralized	3	0.771
	30	1.425
	60	2.034
Scene 3: APs regularly deployed, L2 centralized	3	0.579
	30	1.228
	60	1.796

practical application, the macro station is the center of the grid, where 256 APs are regularly deployed. The ISD is 20 m, which corresponds to the grid size of 320 ∗ 320 m^2. Similarly, the macro station is also the center of the grid, where 255 APs are randomly deployed, and the grid size is 320 ∗ 320 m^2.

Considering that the virtual cell is the direction of the future 5G network, the virtual cell is applied in the simulation scenario. The macro station functions as a control plane service entity, and the APs are the user-plane service entities. Since the service entity is dynamically selected when the UE moves among the APs, the best AP should be chosen by the UE to reduce the connection failure rate and improve the throughput. When the dynamic service AP is selected, for L2 (layer two), the service AP delay is changed to 5 ms. When L1 (layer one) is centralized (to similar RRH), the service AP delay is changed to 0 ms. In crowded scenes, users move relatively slowly. Therefore, we select three low-speed scenes: 3 km/h (on foot), 30 km/h (by bike), and 60 km/h (by car). The handover of the UE among the APs is simulated, as shown in Table 2.

In the simulated scene, when the moving UE accesses APs, the handover frequency is equivalent to the frequency of the communication session's establishment. All data communication sessions need different protection keys. The data protected with a traditional symmetric key method (such as LTE encryption algorithm 128-EEA3) and the key storage space requested for data communication can be calculated by formula (5):

$$\text{Sum}\,(\text{storage}) = \text{length}\,(\text{symmetric\_key}) * \text{times}\,(\text{handover}) \tag{5}$$

For instance, the UE continues moving for 30 minutes with the respective speeds of 3 km/h, 30 km/h, and 60 km/h according to Table 2. The required storage capacity can be calculated using the formula above. The results are shown as follows (assuming the SIM card capacity is 32 kB):

$$128\,\text{bit} * 30 * 60 * 0.731 = 168422\,\text{bits} = 20\,\text{kB} < 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 1.421 = 327398\,\text{bits} = 40\,\text{kB} > 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 2.018 = 464947\,\text{bits} = 56\,\text{kB} > 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 0.771 = 177638\,\text{bits} = 22\,\text{kB} < 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 1.425 = 328320\,\text{bits} = 40\,\text{kB} > 32\,\text{kB}.$$

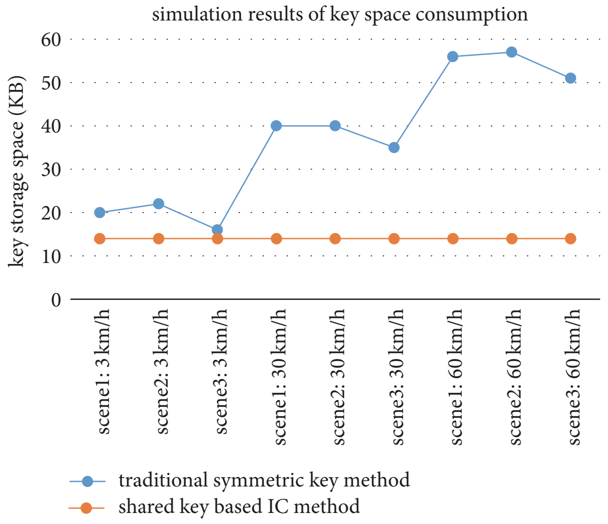


Figure 5: The result of key space consumption.

$$128\,\text{bit} * 30 * 60 * 2.034 = 468634\,\text{bits} = 57\,\text{kB} > 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 0.579 = 133402\,\text{bits} = 16\,\text{kB} < 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 1.228 = 282931\,\text{bits} = 35\,\text{kB} > 32\,\text{kB}.$$

$$128\,\text{bit} * 30 * 60 * 1.796 = 413798\,\text{bits} = 51\,\text{kB} > 32\,\text{kB}.$$

However, in our solution for secure data communication, the pairwise key that includes the public key and private key is a one-off generation using the restructured parameters. The pairwise key should be saved by the network entities, while the shared keys are instantaneously calculated. The shared keys can be generated many times and do not require storage. Therefore, the keys' storage capacity will be basically stable, and the keys' storage space can be calculated by formula (6):

$$\text{Sum}\,(\text{storage}) = \text{length}\,(\text{pairwise\_key}) * \text{quantity}\,(\text{APs}) \tag{6}$$

$225\,\text{bit} * 2 * 256 = 115200\,\text{bits} = 14\,\text{kB}.$

The simulation results of the key storage capacity required are shown in Figure 5.

Figure 5, which is based on Table 2 and formulas (5) and (6), compares the key space consumption under three kinds of UE's speed in traditional symmetric key method and the "shared" key based IC method. In our scenario, by means of the "shared" key based IC method, the key storage space is a constant value, 14 kb, but, with the way of traditional symmetric key method, the key storage space value is dynamic and incremental, which shows that when UE movement rate is greater than 30 km/h, the key storage space is generally greater than 32 KB.

From the above data analysis, we can draw the following conclusions:

(1) The key space consumed by the shared key method based on the IC is significantly less than the space consumption of the traditional symmetric key method.

(2) The key space consumed by the shared key method based on the IC is more stable. In contrast, when using the traditional symmetric key method, the number of protected keys generated by the UE increases with the increasing movement speed.

For 5G UDN, it is very important to have secure and efficient data communications in practical operations. We proposed a scheme where the AKA-IC solution can effectively guarantee the security authentication and data protection among the network entity communication and improve the computational efficiency with less bandwidth.

6. Conclusions

In the 5G, the UDN is an important solution to the explosive growth of network capacity and data traffic. UDN security will directly affect the security of the 5G system. However, there is little research on UDN security. In particular, the data communication security among the network entities of the UDN is still unclear.

In this paper, a new security scheme based on the implicit certificate is introduced based on the analysis of the security challenge of the UDN. We provide the solution that includes the IC and pairwise key generation, and the application process is based on the IC. Then, we analyze the performance of our security communication model. Moreover, an authentication and key agreement protocol based on the IC (AKA-IC) is proposed to solve the secure data communication issue. The AKA-IC algorithm is lightweight and efficient, and the result of the simulated evaluation shows that it is well adapted to various network entities of the UDN, among the APs of APG and between the AP and UE. The security solution based on the IC should be used as an important direction for data communication security for future 5G UDNs.

For future work, in addition to investigating the aforementioned security issues, we also identify other interesting research areas, such as the unified security authentication architecture, the user privacy protection mechanism, and the algorithm optimization of key generation. This will provide more security assurance for 5G systems.

Notations

K:	Symmetric root key for initial authentication
r_U:	Secret random integer generated by entity$U$
R_U:	EC point for the IC request sent by entity$U$
Cert_U:	The implicit certificate of the entity$U$
e:	The result value from the hash computing of Cert_U
s:	The value for the computing private key of the entities
d_U:	The private key of entity$U$
Q_U:	The public key of entity$U$
K_{UV}:	The shared key between entity U and entity V
HMAC:	The keyed-hash message authentication code algorithm.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Zhonglin Chen, Shanzhi Chen, and Hui Xu contributed to the conception and algorithm design of the study. Zhonglin Chen and Hui Xu contributed to the acquisition of simulation. Zhonglin Chen, Hui Xu, and Bo Hu contributed to the analysis of simulation data and approved the final manuscript.

Acknowledgments

This work was supported by the National Science and Technology Major Projects for the New Generation of Broadband Wireless Communication Networks (Grant no. 2016ZX03001017) and the National Natural Science Foundation of China for Distinguished Young Scholars (Grant no. 61425012).

References

[1] S. Chen, "Analysis and Suggestion on Developing 5G," *Telecommunications Science*, vol. 7, pp. 1–10, 2016.

[2] IMT-2020(5G)PG, "WHITE PAPER ON 5G VISION AND REQUIREMENTS_V1.0 [EB/OL]," http://www.imt-2020.cn/zh/documents/1, 2014.

[3] IMT-2020(5G)PG, "WHITE PAPER ON 5G CONCEPT [EB/OL]," http://www.imt-2020.cn/zh/documents/1, 2015.

[4] S. Chen, F. Qin, B. Hu, X. Li, Z. Chen, and J. Liu, *User-Centric Ultra-Dense Networks for 5G*, Springer, Cham, Switzerland, 2017.

[5] Certicom, "Explaining Implicit Certificate," Certicom 2004, Certicom, Mississauga, Canada, 2004.

[6] D. A. Ha, K. T. Nguyen, and J. K. Zao, "Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol," in *SoICT '16: Proceedings of the Seventh Symposium on Information and Communication Technology*, pp. 173–179, ACM, New York, NY, USA, 2016.

[7] P. Porambage, C. Shmitt, P. Kumar, A. Gurtov, and M. Ylianttlila, “Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications,” in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2014–2728, IEEE, Istanbul, Turkey, 2014.

[8] A. P. Hansen, “Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust,” 1999.

[9] Z. F. Tian, “Research on security of public key infrastructure (PKI),” *China Safety Science Journal*, vol. 19, no. 2, pp. 116-117, 2009.

[10] “Wikipedia, the free encyclopedia. Implicit certificate [EB/OL],” https://en.wikipedia.org/wiki/Implicit_certificate, 2017.

[11] C. Gentry, “Certificate-based encryption and the certificate revocation problem,” in *Advances in Cryptology - EUROCRYPT 2003*, E. Biham, Ed., vol. 2656 of *Lecture Notes in Computer Science*, pp. 272–293, Springer, Heidelberg, Germany, 2003.

[12] B. G. Kang, J. H. Park, and S. G. Hahn, “A Certificate-based Signature Scheme,” in *CT-RSA 2004*, T. Okamoto, Ed., vol. 2964 of *Lecture Notes in Computer Science*, pp. 99–111, Springer, Heidelberg, Germany, 2004.

[13] C. Zouridaki, B. L. Mark, K. Gaj, and R. K. Thomas, “Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography,” in *EuroPKI 2004: European Public Key Infrastructure Workshop*, vol. 3093 of *Lecture Notes in Computer Science*, pp. 232–245, Springer, Samos Island, Greece, 2004.

[14] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[15] SEC 4, *Standards for Efficient Cryptography: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)*, Certicom, Mississauga, Canada, 1.2 edition, 2013.

[16] A. Sojka, K. Piotrowski, and P. Langendoerfer, “Short ECC a lightweight security approach for wireless sensor networks,” in *Proceedings of the International Conference on Security and Cryptography, SECRYPT 2010*, pp. 304–308, grc, July 2010.

[17] B. Nair and C. Mala, “Analysis of ECC for application specific WSN security,” in *Proceedings of the 6th IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015*, ind, December 2015.

[18] C. Park, “A Secure and efficient ECQV implicit certificate issuance protocol for the internet of things applications,” *IEEE Sensors Journal*, vol. 17, no. 7, pp. 2215–2223, 2017.

[19] N. M. Rabadi, “Improved anonymous group implicit certificate scheme,” in *Proceedings of the 2011 IEEE Consumer Communications and Networking Conference, CCNC'2011*, pp. 308–312, usa, January 2011.

[20] B. Vaidya, D. Makrakis, and H. Mouftah, “Effective public key infrastructure for vehicle-to-grid network,” in *Proceedings of the 4th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, DIVANet 2014*, pp. 95–101, can, September 2014.

[21] Li. Yue and P. Mugen, “Layered heterogeneous wireless networking scheme based on virtual cell,” *Telecommunications Science*, vol. 1, pp. 8–12, 2013.

[22] S. Chen, F. Qin, B. Hu, X. Li, and Z. Chen, “User-centric ultra-dense networks for 5G: Challenges, methodologies, and directions,” *IEEE Wireless Communications Magazine*, vol. 23, no. 2, pp. 78–85, 2016.

[23] Z. Chen, S. Chen, H. Xu, and B. Hu, “Security architecture and scheme of user-centric ultra-dense network (UUDN),” *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 9, Article ID e3149, 2017.

[24] H. Kaizhi, J. Liang, and Z. Hua, “Research on 5G security threat and protection technologies,” *Designing Techniques of Posts and Telecommunications*, vol. 6, pp. 8–12, 2015.

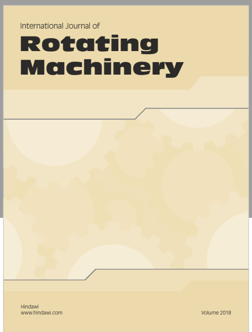
[25] H. Mun, K. Han, and K. Kim, “3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA,” in *Proceedings of the 2009 Wireless Telecommunications Symposium, WTS 2009*, cze, April 2009.

[26] Y. Park and T. Park, “A Survey of Security Threats on 4G Networks,” in *Proceedings of the 2007 IEEE Globecom Workshops*, pp. 1–6, Washington, DC, USA, November 2007.

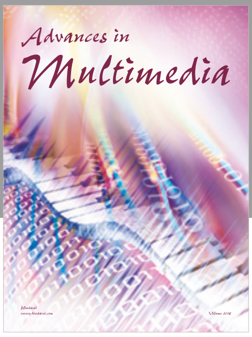
[27] M. Peng, Y. Li, Z. Zhao, and C. Wang, “System architecture and key technologies for 5G heterogeneous cloud radio access networks,” *IEEE Network*, vol. 29, no. 2, pp. 6–14, 2015.

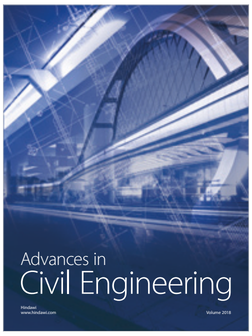
Journal of
Engineering

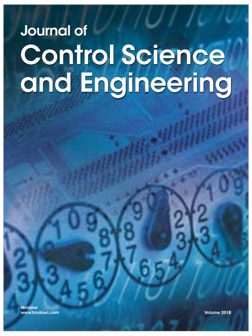
The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

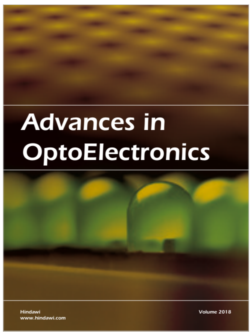

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

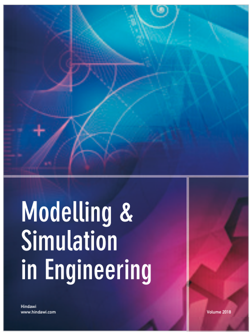
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

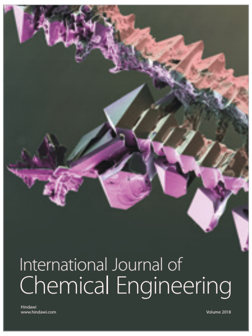

Advances in
OptoElectronics

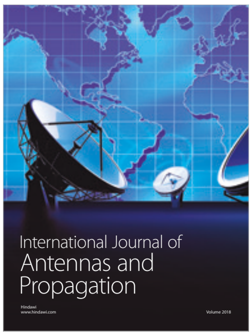
VLSI Design

International Journal of
Navigation and
Observation

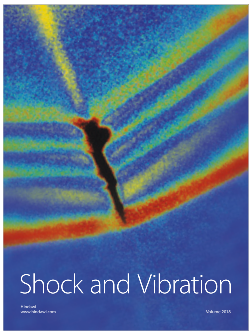

Modelling &
Simulation
in Engineering

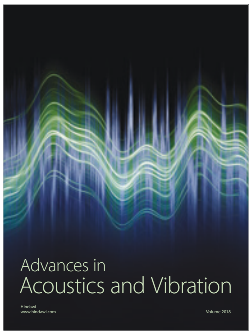
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration